

REMARKS

This Application has been carefully reviewed in light of the Office Action mailed September 19, 2006. Claims 1-26 were pending in the Application. In the Office Action, Claims 1-26 were rejected. Claims 1-26 remain pending in the Application. Applicants respectfully request reconsideration and favorable action in this case.

In the Office Action, the following actions were taken or matters were raised:

SECTION 102 REJECTIONS

Claims 1-17, 19-24 and 26 were rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,978,475 issued to Schneier et al. (hereinafter "*Schneier*"). Claims 1, 10 and 19 are rejected under 35 USC §102(e) as being anticipated by U.S. Patent No. 6,088,804 issued to Hill et al. (hereinafter "*Hill*"). Applicants respectfully traverse these rejections.

Schneier Reference

Of the rejected claims, Claims 1, 10 and 19 are independent. Applicants respectfully submit that *Schneier* does not disclose or even suggest each and every limitation of independent Claims 1, 10 and 19. *Schneier* appears to disclose an untrusted computer 102 (which the Examiner appears to consider as the "target" recited by Claim 1) having an audit logging program 200 for generating an audit log 300 (*Schneier*, column 4, lines 13-61). The Examiner appears to consider the audit log 300 of *Schneier* as corresponding to the "probe" recited by Claim 1 (Office action, page 3). However, the Examiner's reliance appears misplaced at least because Claim 1 recites that the probe is "operable to execute in the target" (emphasis added). Accordingly, because the audit log 300 of *Schneier* does not appear to be executable, Applicants presume that the Examiner intends the audit logging program 200 of *Schneier* to correspond to the "probe" recited by Claim 1, and that the Examiner considers the audit log 300 of *Schneier* as corresponding to the "predetermined set of data" that is

collected by the probe as recited by Claim 1. Applicants respond to this rejection based on the foregoing.

Schneier appears to be directed toward generating a secure audit log 300 by the untrusted computer 102 of *Schneier* (*Schneier*, column 3, lines 6-19). For example, *Schneier* appears to disclose a cryptographic module 220 that is used in combination with the audit logging program 200 to protect the audit log 300 (*Schneier*, column 6, lines 12-21). *Schneier* also appears to disclose a trusted computer 101 and/or a verifier computer 103 that may be used to verify the audit log 300 (*Schneier*, column 13, lines 4-25). Thus, *Schneier* appears to be directed toward determining whether the audit log 300 has been tampered with or altered. Thus, based on the foregoing, the *Schneier* reference appears to be directed toward determining whether the "predetermined set of data" (the audit log 300) is altered, instead of whether the untrusted computer 102 (the "target") has been altered. Accordingly, for at least this reason, Applicants respectfully submit that *Schneier* does not disclose or even suggest "a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered" as recited by Claim 1 (emphasis added).

Independent Claim 10 recites "collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered" (emphasis added), and independent Claim 19 recites "comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered" (emphasis added). Accordingly, for at least the reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that *Schneier* also does not anticipate independent Claims 10 and 19.

Claims 2-9, 11-17, 20-24 and 26 that depend respectively from independent Claims 1, 10 and 19 are also not anticipated by *Schneier* at least because they incorporate the limitations of respective Claims 1, 10 and 19 and also add additional elements that further distinguish *Schneier*. Therefore, Applicants respectfully request that the rejection of Claims 1-17, 19-24 and 26 in view of *Schneier* be withdrawn.

Hill Reference

Of the rejected claims, Claims 1, 10 and 19 are independent. Applicants respectfully submit that *Hill* does not disclose or even suggest each and every limitation of independent Claims 1, 10 and 19. For example, *Hill* appears to disclose a security agent 36 (which the Examiner appears to consider to correspond to the "probe" recited by Claim 1) that detects occurrences of security events on a computer node (e.g., port scans, malicious software being operated on the node, and penetration attempts) (*Hill*, abstract, column 4, lines 30-41, column 10, lines 24-36). *Hill* also appears to disclose a SOM processor 40 that receives the security events from the security agent 36 of *Hill* and forms an attack signature that the SOM processor 40 then compares to training signatures to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36).

In the Office Action, the Examiner does not explicitly identify what the Examiner considers in *Hill* to correspond to the "monitor" recited by Claim 1. However, because the SOM processor 40 appears to be used in *Hill* to compare an attack signature to training signatures, and at least because the Examiner states that "agents send info. for collection and comparison" (Office Action, page 5), Applicants presume that the Examiner intends that the SOM processor 40 of *Hill* correspond to the "monitor" recited by Claim 1. Based on the foregoing, Applicants respectfully submit that the SOM processor 40 of *Hill* does not compare an attack signature to training signatures in *Hill* "to determine whether the target has been altered" as recited by Claim 1. To the contrary, the SOM processor 40 of *Hill* appears to make the above-referenced comparison to determine a recommended action or response to an attack. Accordingly,

for at least this reason, Applicants respectfully submit that *Hill* does not anticipate Claim 1.

Independent Claim 10 recites "collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered" (emphasis added), and independent Claim 19 recites "comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered" (emphasis added). Accordingly, for at least the reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that *Hill* also does not anticipate independent Claims 10 and 19.

SECTION 103 REJECTIONS

Claims 18 and 25 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Schneier*. Applicants respectfully traverse this rejection.


Claims 18 and 25 depend respectively from Claims 10 and 19. At least for the reasons discussed above, Claims 10 and 19 are in condition for allowance. Therefore, Claims 18 and 25 that depend respectively therefrom are also allowable, and Applicants respectfully request that the rejection of Claims 18 and 25 be withdrawn.

CONCLUSION

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicants have overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By: 
James L. Baudino
Reg. No. 43,486

Date: December 5, 2006

Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400
Tel. 970-898-3884